ALIDADE
INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

For 9th ICCRTS
Copenhagen, Denmark
September 16th, 2004

By: David Garvey
Presented By: David A. Jarvis

Originally for the Smith-Richardson Foundation monograph on
"Defeating Global Terrorism, Securing the Port of New York and New Jersey"

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **SEP 2004**	2. REPORT TYPE	3. DATES COVERED **00-00-2004 to 00-00-2004**
4. TITLE AND SUBTITLE **Possible Applications of Distributed, Networked Architectures to Port Security**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Alidade Incorporated,31 Bridge Street,Newport,RI,02840**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**18**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Agenda

- Introduction
- Basic Questions
- Applying Net-Centric Operations to Port Security
- Adaptation vs. Optimization
- Port Security Modeled as a Complex Network
- Important Complex Network Properties and Considerations
- Application of Network Properties to Commerce Flow Networks
- Conclusions
- Recommendations

Possible Applications of Distributed, Networked Architectures to Port Security

Introduction

- Paper in support of the Stevens Technology Institute and the New York/New Jersey Port Authority (NNPA)
- Looking for new management and communications models, better public/private cooperation, rapid collection and analysis of data, and to provide prevention and rapid response
- Goal was to apply network-centric management concepts to the problem of securing ports
- Alidade provided military experience applying NCO principles

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Port of NY and NJ; ~18 by 25 miles = 450 sq. miles ~15-17 million

ALIDADE
INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Basic Questions

- Complex networks have exploitable properties
  - What relevance do they have in a homeland defense and port defense context?
- In support of a distributed, networked architecture for port security:
  - What are the defining mathematical characteristics of a distributed, networked system in the Information Age?
  - What should a distributed, networked system be capable of?
  - How should distributed, networked systems be developed to exploit their full potential?

ALIDADE INCORPORATED

Applying Network-Centric Operations to Port Security

- Four tenets of NCO
  - Robustly networked force improves information sharing
  - Which increases the "quality" of information and shared situational awareness
  - This enables collaboration and self-synchronization, while enhancing sustainability and speed of command
  - Which leads to increased mission capabilities
- There are two often overlooked requirements that emerge from the adoption of the above tenets
  - Co-evolution and complex landscapes
  - Limitations of information sharing

ALIDADE INCORPORATED

Applying Network-Centric Operations to Port Security

- Co-evolution
  - U.S. Homeland Security forces and agencies at the local, state and federal level (Blue) are linked via non-linear feedback loops to opponents wishing to cause harm inside U.S. borders (Red)
  - The co-evolution of Blue and Red strategies creates a dynamic landscape that makes traditional modeling difficult
- Information sharing
  - The National Security Strategy for Homeland Security, DoD CIO, and the Markle Foundation Homeland Security Task Force all emphasize the importance of seamless information sharing
  - In and of itself does not enable network-centric effects, "information overload" can actually degrade decision making processes, leads to over-reliance on technology
  - New processes and structures must be created that match the topology of the physical and information flows, just overlaying IT on top of old processes is not cost effective and does not generate new capability

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Adaptation vs. Optimization

- Commercial port systems are structured to enable the flow of goods in such a way to maximize profit and minimize amount of time in the system (optimized system)
- No Free Lunch Theorem of Optimization
  - In the absence of information from the environment a single optimization algorithm cannot be the best for all types of problems (Wolpert and Macready)
- Good adaptive processes find a balance between:
  - Exploration (learning about the environment)
  - Exploitation (applying what is learned to the search for a better solution)
- Even though optimization algorithms might be employed during adaptation, adaptation typically does not usually produce a global optimum
- The structure of a "commerce flow network" must be designed to be adaptive, allowing enough slack in the system to absorb perturbations
- To be resilient to attack the commerce flow network needs to have extra structure than the necessary minimum (neutrality), which comes with a higher initial investment cost

ALIDADE
INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Port Security Modeled as a Complex Network

- In order to design a port security solution that is adaptive and resilient to attack, must think of the port system as a complex network
  - Diverse elements networked together and interacting via nonlinear feedback cycles
  - What is a node?
    - Both Red and Blue, containerized cargo (legitimate and contraband), key decision makers (defenders and attackers), initial responders, piers, warehouses, trucks, trains and ships
  - What is a link?
    - Observations from a perimeter, declaration of emergency incidents, inspections and boardings, transfer between transportation nodes

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Important Complex Network Properties and Considerations

- Networks have a form that is driven by their function
- Important Network Properties
  - ***Largest hub:*** How big a component surrounds the most connected node? By rerouting only ~5-10% of the links, the giant component can appear, relocated and recede entirely
  - ***Degree distribution:*** how many nodes have how many links, a representation of the connection pattern of a network
  - ***Characteristic path length (CPL):*** the median of the average distance from each node to every other node in the network
  - ***Clustering:*** a measure of local cohesion in a network, measures the extent to which nodes that are connected to a particular node are also connected to each other
  - ***Susceptibility/Resilience/Robustness:*** the extent a network can avoid catastrophic failure as links or nodes are removed and how other properties are affected by node/link removal
  - ***Betweenness:*** measure of a node's importance to dynamic behaviors in a complex network, measures the number of shortest paths that pass through a node
  - ***Path horizon:*** measure of how many nodes, on average, that a node must interact with for constructive self-synchronization to occur, how many nodes away is each node aware of
  - ***Neutrality:*** the amount of "excess structure" in a network
- Network Considerations
  - ***Structure:*** The definition of links, nodes and their possible connections
  - ***Dynamics:*** Feed-back or feed-forward links that create network effects
  - ***Evolution:*** Long-term statistics as the network fulfills its purpose

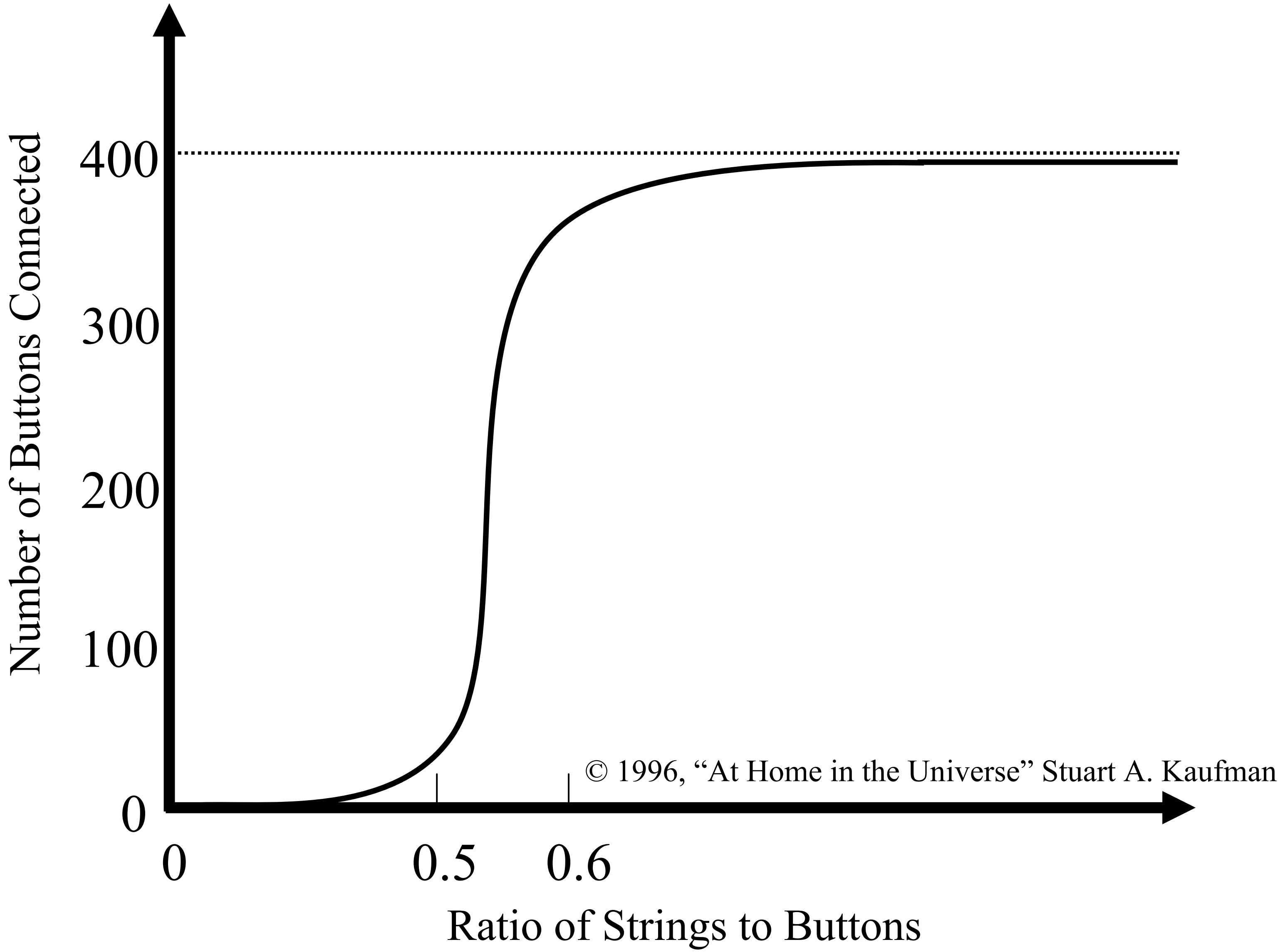
ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Complex Network Properties Applied to Commerce Flow Networks

- Betweenness
  - Since search assets are currently scarce, target those hubs that have the highest betweenness
- Neutrality and risk management
  - With limited resources can't stop all penetrations of the commerce network; mitigate, reroute and reconfigure the system using neutral structure if a hub is attacked
- Preventing cascade failures
  - Removal of key hubs can overload other nodes in the network, design the commerce flow network and associated command and control structures to prevent failure from percolating throughout the system (by removing key links at key times)

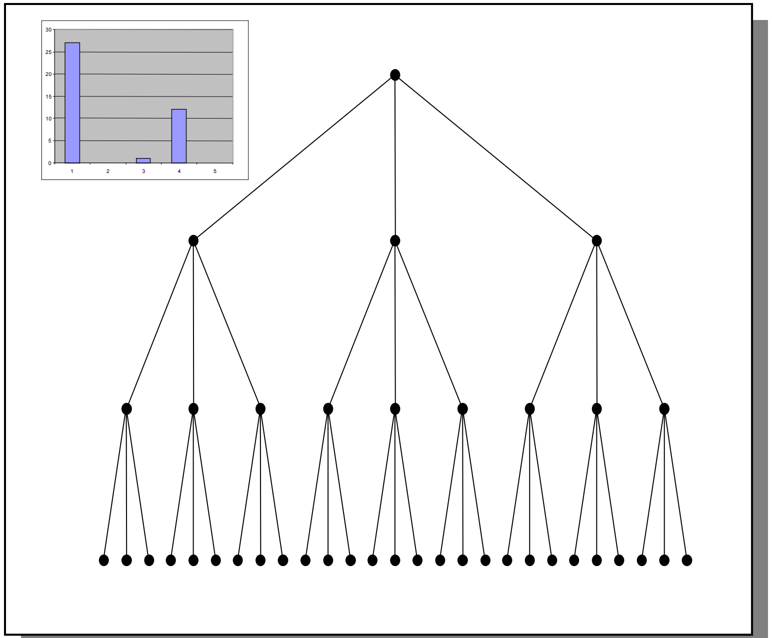
Complex Network Properties

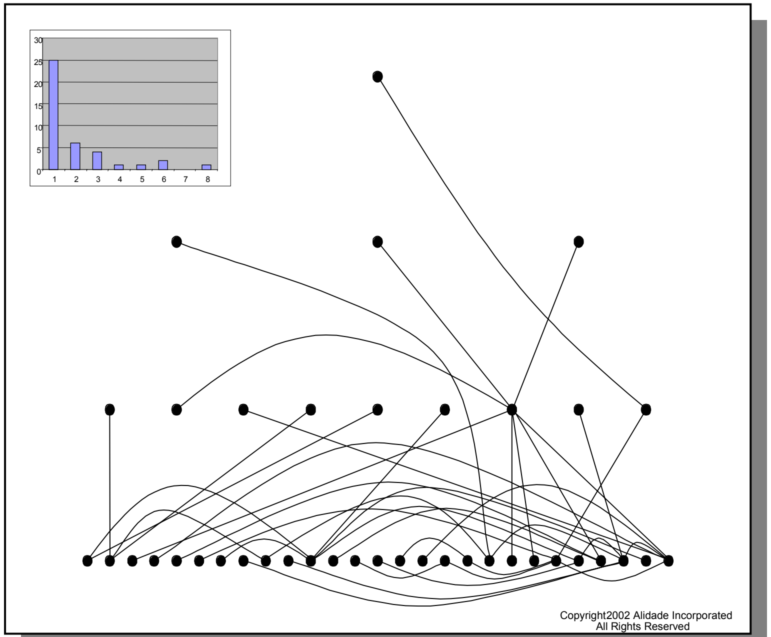


ALIDADE
INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Complex Network Properties
Chains v. Networks





Assumed Model

Too brittle, long paths, low clustering, simple pattern, simple control, scaled

“business end” most poorly connected, hard to reconfigure or change flow

Actual Behavior

Very robust, short paths, “skew” clustering, complex pattern, complex control, scale free

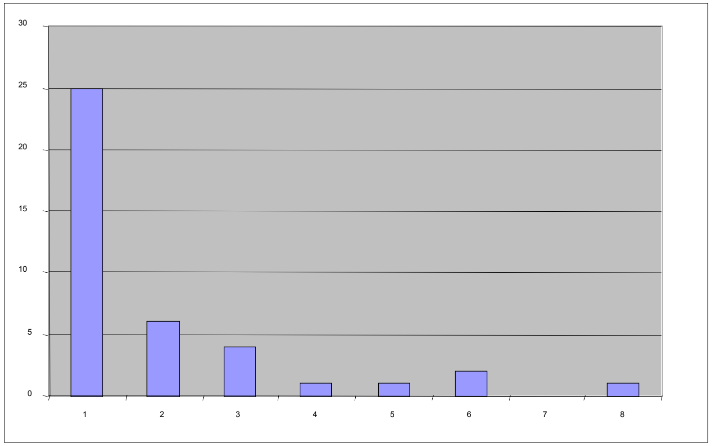
“business end” best connected, natural to reconfigure or change flow

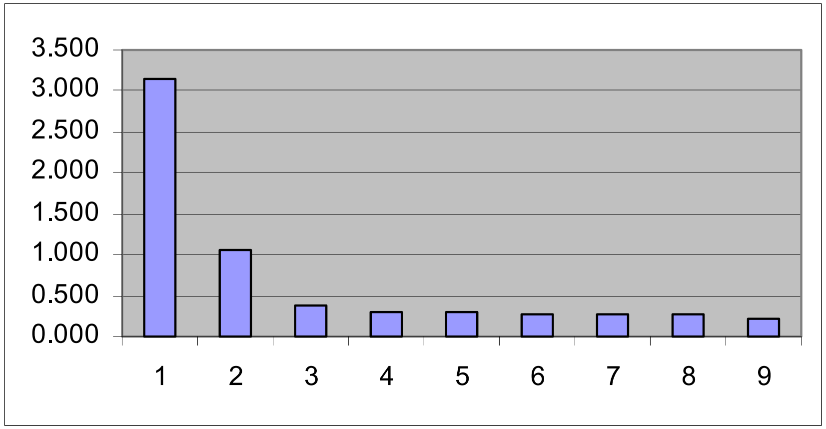
9th ICCRTS

September 16th, 2004

Possible Applications of Distributed, Networked Architectures to Port Security

Similarities Observed:
Something more than coincidence?





"Small world network" degree distribution plot from previous page

Top ten US ports (LA+LB combined) by number of containers

Thumb Rules

Analysis and Experimentation

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Property	Range	Effect
Number of nodes, n	$n > \sim 100$	Network effects unlikely to occur with n < 50
Number of links, l	$l < \sim 2n$	$l << 2n$, too brittle $l >> 2n$, too much overhead
Degree distribution	Skewed	Adaptivity, modularity
Largest hub	< 100 links	Hub appears, recedes by reconnection 5% of links
Average path length	$\log(n)$	Short distances even for large networks (e.g., 10^4 nodes → Average path length = ~4)
Clustering	Skewed	Hierarchy, organization
Between-ness	Skewed	Cascade control
Path horizon	$\log(n)$	Self-synchronization
Susceptibility/ Robustness	Low (random removal) High (focused removal)	Hubs should be kept obscure until needed, damage abatement/repair schemes
Neutrality	High	Increased network effects, decreased susceptibility, tipping points

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Conclusions

- Cursory observation indicates commerce flow through ports behaves mathematically as a “complex, adaptive, networked system”
- If this is true, then there are exploitable properties of real world networks that should be used as design principles
- Only experimentation (as opposed to exercises) will give policy insight into how much “network neutrality” is required

ALIDADE INCORPORATED

Possible Applications of Distributed, Networked Architectures to Port Security

Recommendations

- Experiments must be done to map network structure of commerce flow in NNPA
- Front-end costs of network neutrality must be advertised as buying new capability
  - Just applying IT to existing processes is not a sound economic decision
- A level of tolerance must be found for divestment of direct control over flows
  - Global vs. local optimums
- How much of the above analysis will be open source available to attackers?

ALIDADE
INCORPORATED

Complex Systems Research

Process Innovation & Analysis

Strategic Investment Advice

Future Concept Generation

Corporate/Government War Games & Events

Questions?